

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

IRENE CHABAK, ARMANDO
CARRASCO, RANDY POLK, KELLY
WILSON, THOMAS BOOTH HARRIS,
SCOTT WEISCOPE, LAVINA
HENDERSON, and JEREMY
HENDERSON, *individually and on behalf of*
all others similarly situated,

Plaintiffs,

v.

SOMNIA INC., ANESTHESIA SERVICES
OF SAN JOAQUIN P.C., PALM SPRINGS
ANESTHESIA SERVICES P.C.,
RESOURCE ANESTHESIOLOGY
ASSOCIATES OF IL P.C., RESOURCE
ANESTHESIOLOGY ASSOCIATION OF
NM INC., and ANESTHESIA ASSOCIATES
OF EL PASO, P.A.,

Defendants.

Case No.: 7:22-cv-9341-PMH

**FIRST CONSOLIDATED AMENDED
COMPLAINT**

JURY TRIAL DEMANDED

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION & SUMMARY OF THE COMPLAINT	1
II. JURISDICTION AND VENUE	5
III. NAMED PLAINTIFFS.....	7
A. CALIFORNIA	7
1. Raycine Sommers	7
2. Randy Polk.....	9
3. Kelly Wilson	10
4. Thomas Booth Harris	11
B. TEXAS.....	13
1. Irene Chabak	13
2. Armando Carrasco	14
C. ILLINOIS.....	15
1. Scott Weiscope.....	15
D. NEW MEXICO.....	16
1. Lavina Henderson	16
2. Jeremy Henderson.....	18
IV. DEFENDANTS	19
A. SOMNIA, INC.....	19
B. ANESTHESIA SERVICES OF SAN JOAQUIN, P.C.....	19
C. PALM SPRINGS ANESTHESIA SERVICES, P.C.	19
D. RESOURCE ANESTHESIOLOGY ASSOCIATES OF IL, P.C.....	19
E. RESOURCE ANESTHESIOLOGY ASSOCIATES OF NM INC.	20
F. ANESTHESIA ASSOCIATES OF EL PASO, P.A.	20
V. FACTUAL ALLEGATIONS	20
A. DEFENDANTS' COLLECTION OF PERSONAL INFORMATION.	20
B. THE DATA BREACH.	21
C. DEFENDANTS' NOTICE WAS DEFICIENT.....	23
D. DEFENDANTS FAILED TO SAFEGUARD PERSONAL INFORMATION.....	24
E. DEFENDANTS VIOLATED REGULATORY GUIDANCE AND HIPAA'S REQUIREMENTS TO SAFEGUARD DATA.	27

TABLE OF CONTENTS
(Cont'd)

	<u>Page</u>
F. PLAINTIFFS' AND CLASS MEMBERS' PERSONAL INFORMATION IS HIGHLY VALUABLE	30
G. DEFENDANTS HARMED PLAINTIFFS AND CLASS MEMBERS BY ALLOWING ANYONE TO ACCESS THEIR PERSONAL INFORMATION.....	33
H. HACKERS SOLD CLASS MEMBERS' PERSONAL INFORMATION ON THE DARK WEB.....	38
CLASS ACTION ALLEGATIONS	39
A. CLASS DEFINITIONS	39
1. NATIONWIDE CLASS	39
2. THE DEFENDANT ANESTHESIOLOGY PROVIDER-SPECIFIC SUBCLASSES.....	39
3. STATEWIDE SUBCLASSES.....	40
B. THE PROPOSED CLASSES MEET THE RELEVANT RULE 23 REQUIREMENTS.....	40
CLAIMS ON BEHALF OF THE NATIONWIDE CLASS	45
COUNT 1 NEGLIGENCE	45
COUNT 2 NEGLIGENCE PER SE	49
COUNT 3 BREACH OF CONFIDENCE.....	51
COUNT 4 UNJUST ENRICHMENT	52
CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS.....	55
COUNT 5 CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT Cal. Civ. Code §§ 56, <i>et seq.</i>	55
COUNT 6 CALIFORNIA UNFAIR COMPETITION LAW Cal. Bus. & Prof. Code §§ 17200, <i>et seq.</i>	59
COUNT 7 CALIFORNIA CONSUMER LEGAL REMEDIES ACT Cal. Civ. Code §§ 1750, <i>et seq.</i>	61
COUNT 8 CALIFORNIA CONSUMER RECORDS ACT Cal. Civ. Code §§ 1798.80, <i>et seq.</i>	64
REQUESTS FOR RELIEF	65
DEMAND FOR JURY TRIAL	66

Plaintiffs, individually and on behalf of all those similarly situated (the “Classes” or “Class Members”) make the following allegations with personal knowledge of the facts about Plaintiffs themselves and on information and belief as to all other matters based on Counsel’s investigation. Because Defendants have exclusive but perhaps incomplete knowledge of what information was compromised for each individual, Plaintiffs reserve the right to supplement their allegations with additional Plaintiffs, facts, and injuries as they are discovered.

I. INTRODUCTION & SUMMARY OF THE COMPLAINT

1. On or about July 11, 2022, Defendant Somnia, Inc. (“Somnia”) belatedly detected hackers within its systems (the “Data Breach”). These unauthorized attackers intentionally compromised Somnia’s systems and made off with Plaintiffs’ and Class Members’ names, dates of birth, driver’s license numbers, Social Security numbers, financial account information, health insurance policy numbers, Medical Record Numbers, Medicaid or Medicare IDs, and health information such as treatment and diagnostic information.

2. Somnia is an anesthesiology services provider and practice management company that manages numerous anesthesiology providers, including Defendants Anesthesia Services of San Joaquin P.C. (“AS-San Joaquin”), Palm Springs Anesthesia Services P.C. (“Palm Springs-AS”), Resource Anesthesiology Associates of IL P.C. (“RAA-IL”), Resource Anesthesiology Association of NM Inc. (“RAA-NM”), and Anesthesia Associates of El Paso, P.A. (“AA-El Paso”) (collectively, “the Defendant Anesthesiology Providers”). Somnia obtains numerous individuals’ personally identifiable information (“PII”) and private health information (“PHI”) (collectively, “Personal Information”) from its anesthesiology providers, including the Defendant Anesthesiology Providers.

3. While Somnia has not been forthcoming about the details of the Data Breach, its system was compromised by attackers such that it required “a global password reset, tightening

firewall restrictions, and implementing endpoint threat detection and response monitoring software on workstations and servers.” These myriad remediation measures demonstrate the breadth of the deficiencies within Somnia’s system. Unsurprisingly given the overwhelming security failures, Plaintiffs were informed that “[Somnia’s] investigation found that some information stored on the management company’s systems may have been compromised.”

4. On or about October 24, 2022, fifteen anesthesiology practices across the country announced that their patients’ information was part of the Data Breach involving their unnamed “management company,” subsequently revealed to be Somnia. On November 7, 2022, additional anesthesiology practices announced that their patients were also victims of the Data Breach.

5. As of this filing, more than 450,000 individuals’ information was taken in the Data Breach.

Anesthesiology Provider	Individuals Affected
Providence WA Anesthesia Services	98,643
Palm Springs Anesthesia Services	58,513
Anesthesia Services of San Joaquin	44,015
Anesthesia Associates of El Paso	43,168
Resource Anesthesiology Associates PC	37,687
Resource Anesthesiology Associates of IL	18,321
Bronx Anesthesia Services	17,802
Resource Anesthesiology Associates of CA	16,001
Grayling Anesthesia Associates	15,378
Hazleton Anesthesia Services	13,607
Anesthesia Associates of Maryland	12,403

Anesthesiology Provider	Individuals Affected
Somnia Pain Mgt of Kentucky	10,849
Primary Anesthesia Services	9,517
Upstate Anesthesia Services	9,065
Resource Anesthesiology Associates of KY	8,980
Saddlebrook Anesthesia Services	8,861
Fredericksburg Anesthesia Services	7,069
Lynbrook Anesthesia Services	3,800
Resource Anesthesiology Associates of VA	3,305
Resource Anesthesiology Associates of CT PC	3,123
Somnia, Inc.	1,326
Resource Anesthesiology Associates of CA PC	1,308
Mid-Westchester Anesthesia Services	707
Total	450,512¹

6. The Defendant Anesthesiology Providers, and the other anesthesiology providers listed above, negligently entrusted their customers' Personal Information to Somnia.

7. Defendants have a duty to safeguard and protect customer information entrusted to them and could have prevented this theft by, in the case of Somnia, implementing adequate security measures and, in the case of the Defendant Anesthesiology Providers, limiting the customer information shared with vendors and business associates.

¹ *Data Breach Impacts Two Dozen Anesthesia Providers*, Oct. 13, 2022, available at <https://www.hipaajournal.com/data-breach-impacts-more-than-one-dozen-anesthesia-providers/> (accessed Feb. 27, 2023).

8. Plaintiffs and Class Members entrusted Defendants with, and allowed Defendants to gather, highly sensitive information relating to their health and other matters as part of seeking medical treatment. They did so in confidence, with the legitimate expectation that Defendants would respect their privacy and act appropriately, including only sharing their information with vendors and business associates who were equipped to protect it.

9. Trust and confidence are key components of Defendants' relationship with Plaintiffs and Class Members. Without that trust and confidence, Plaintiffs and Class Members would not have provided Defendants with, or allowed Defendants to collect, their most sensitive information in the first place; Plaintiffs and Class Members relied upon Defendants to keep their information secure (as Defendants are required by law to do).

10. Plaintiffs bring this class action because Defendants collected but failed to secure and safeguard numerous anesthesiology patients' Personal Information—such as Plaintiffs' and Class Members' names, dates of birth, driver's license numbers, financial account information, health insurance policy numbers, Medical Record Numbers, Medicaid or Medicare IDs, and health information such as treatment and diagnostic information.

11. More than 450,000 anesthesiology patients had their Personal Information compromised in the Data Breach. As a result of Defendants' failure to protect the consumer information they were entrusted to safeguard, Plaintiffs and Class Members suffered a loss of the value of their Personal Information, and have been exposed to or are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future.

12. In fact, by July 21, 2022, Class Members' Personal Information was being sold on

the dark web.²

13. Defendants' intentional, willful, reckless, unfair, and negligent conduct—failing to prevent the breach, failing to limit its severity, and failing to detect it in a timely fashion—harmed Plaintiffs and Class Members uniformly. For this reason, Defendants should pay for monetary damages and appropriate identity theft protection services, as well as reimburse Plaintiffs for the costs caused by Defendants' substandard security practices and failure to timely disclose the same. Plaintiffs are likewise entitled to injunctive and other equitable relief that safeguards their information, requires Defendants to improve their data security significantly, and provides independent, expert oversight of Defendants' security systems.

14. Defendants have also been unfairly and unjustly enriched because of their improper conduct, such that it would be inequitable for them to retain the benefits conferred upon them by Plaintiffs and the Class Members. Plaintiffs never would have engaged their anesthesiology providers to perform medical services and entrusted Defendants with their Personal Information, had they known that Defendants would permit unauthorized access to their Personal Information because of Defendants' complete and utter disregard for security safeguards and protocols. Plaintiffs would have used other providers.

II. JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of \$5,000,000, there are more than 100 Class Members, and minimal diversity exists as Defendants are citizens of States different from that of at least one Class Member.

² The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it* (Apr. 14, 2018), <https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html> (last accessed Feb. 22, 2023).

16. This Court has personal jurisdiction over Somnia because it maintains its principal place of business in this District. Somnia is authorized to and regularly conducts business in New York. Somnia makes decisions regarding corporate governance and management of its business in this District, including decisions regarding the security measures to protect its customers' Personal Information.

17. This Court has personal jurisdiction over AS-San Joaquin because it regularly conducts business in New York and has sufficient minimum contacts in New York such that it intentionally avails itself of this Court's jurisdiction by conducting operations here and contracting with companies in this District.

18. This Court has personal jurisdiction over Palm Springs-AS because it regularly conducts business in New York and has sufficient minimum contacts in New York, including its business address being in New York, such that it intentionally avails itself of this Court's jurisdiction by conducting operations here and contracting with companies in this District.

19. This Court has personal jurisdiction over RAA-IL because it regularly conducts business in New York and has sufficient minimum contacts in New York, including its business address being in New York, such that it intentionally avails itself of this Court's jurisdiction by conducting operations here and contracting with companies in this District.

20. This Court has personal jurisdiction over RAA-NM because it regularly conducts business in New York and has sufficient minimum contacts in New York, including its business address being in New York, such that it intentionally avails itself of this Court's jurisdiction by conducting operations here and contracting with companies in this District.

21. This Court has personal jurisdiction over AA-El Paso because it regularly conducts business in New York and has sufficient minimum contacts in New York, including its business

address being in New York, such that it intentionally avails itself of this Court's jurisdiction by conducting operations here and contracting with companies in this District.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because each Defendant transacts business and may be found in this District. Specifically, Somnia's principal place of business is located in this District and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Defendants' governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the Data Breach. Further, all of the Defendant Anesthesiology Providers have New York mailing addresses.

III. NAMED PLAINTIFFS

23. Plaintiffs are individuals who had their Personal Information compromised in the Data Breach. Each suffered a concrete and particularized injury because of Defendants' failure to protect their Personal Information and the subsequent disclosure of their Personal Information to unauthorized parties without their consent.

24. Had Defendants disclosed that they disregarded their duty to safeguard and protect Plaintiffs' Personal Information from unauthorized access, Plaintiffs would have taken that into account in making their healthcare decisions. In particular, had Plaintiffs known about Somnia's failure to safeguard their Personal Information, they would not have provided their Personal Information to Defendants.

A. CALIFORNIA

1. Raycine Sommers

25. Plaintiff Raycine Sommers is a natural person residing in Stockton, California. She is a citizen of California.

26. Plaintiff Sommers received anesthesia as part of surgeries in a California hospital

in November 2019, February 2020, and July 2021.

27. Plaintiff Sommers has no known relationship with Defendants other than having surgeries under anesthesia and receiving a breach notice from AS-San Joaquin on or around October 24, 2022.

28. In order to receive healthcare services, Plaintiff Sommers had to provide her Personal Information to AS-San Joaquin.

29. Plaintiff Sommers did so and, upon information and belief, AS-San Joaquin passed her information along to Somnia. Plaintiff Sommers trusted that Somnia and AS-San Joaquin would use reasonable measures to protect her information, including complying with state and federal law.

30. Plaintiff Sommers suffered harm as a result of the Data Breach. For example, she spent time verifying the legitimacy of the breach notice, exploring credit monitoring, and placing an Experian fraud alert on her account.

31. Plaintiff Sommers also faced a litany of identity theft since she provided her information to Defendants. For example, in August 2022, Plaintiff Sommers received a spam call informing her that a freeze was being placed on her Bank of America account. In October 2022, Plaintiff Sommers received a fraudulent text message that one of her credit cards was blocked. In November 2022, Plaintiff Sommers got an alert that she had voted in an election in Florida, despite not doing so and being a California resident.

32. Plaintiff Sommers is aware of no other source from which the theft of her Personal Information could have come. She regularly takes steps to safeguard her Personal Information in her own control.

33. Plaintiff Sommers suffered actual injury in the form of damages to and diminution

of the value of her Personal Information, which she entrusted to Defendants and which was compromised in the Data Breach.

34. Plaintiff Sommers suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her Personal Information because that information was accessed and exfiltrated by hackers. This injury was exacerbated by Defendants' delay in revealing the Data Breach.

35. Plaintiff Sommers has a continuing interest in ensuring that her Personal Information, which remains with Defendants, is protected and safeguarded from future breaches.

2. Randy Polk

36. Plaintiff Randy Polk is a natural person residing in Los Angeles, California. He is a citizen of California.

37. Plaintiff Polk received anesthesia as part of a medical procedure in October 2021.

38. Plaintiff Polk has no known relationship with Defendants other than having surgeries under anesthesia and receiving a breach notice from Palm Springs-AS on or around October 24, 2022.

39. In order to receive healthcare services, Plaintiff Polk had to provide his Personal Information to Palm Springs-AS.

40. Plaintiff Polk did so and, upon information and belief, Palm Springs-AS passed his information along to Somnia. Plaintiff Polk trusted that Somnia and Palm Springs-AS would use reasonable measures to protect his information, including complying with state and federal law.

41. Plaintiff Polk suffered harm as a result of the Data Breach. For example, he spent time verifying the legitimacy of the breach notice, contacting Defendants regarding the Data Breach, and exploring options to deal with the exposure of his Personal Information in the Data Breach.

42. Plaintiff Polk is aware of no other source from which the theft of his Personal Information could have come. He regularly takes steps to safeguard his Personal Information in his own control.

43. Plaintiff Polk suffered actual injury in the form of damages to and diminution of the value of his Personal Information, which he entrusted to Defendants and which was compromised in the Data Breach.

44. Plaintiff Polk suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his Personal Information because that information was accessed and exfiltrated by hackers. This injury was exacerbated by Defendants' delay in revealing the Data Breach.

45. Plaintiff Polk has a continuing interest in ensuring that his Personal Information, which remains with Defendants, is protected and safeguarded from future breaches.

3. Kelly Wilson

46. Plaintiff Kelly Wilson is a natural person residing in Rialto, California. She is a citizen of California.

47. Plaintiff Wilson received anesthesia as part of a surgery in a California hospital in April 2019.

48. Plaintiff Wilson has no known relationship with Defendants other than having surgeries under anesthesia and receiving a breach notice from Palm Springs-AS on or around October 27, 2022.

49. In order to receive healthcare services, Plaintiff Wilson had to provide her Personal Information to Palm Springs-AS.

50. Plaintiff Wilson did so and, upon information and belief, Palm Springs-AS passed her information along to Somnia. Plaintiff Wilson trusted that Somnia and Palm Springs-AS would

use reasonable measures to protect her information, including complying with state and federal law.

51. Plaintiff Wilson suffered harm as a result of the Data Breach. For example, she spent time verifying the legitimacy of the breach notice, contacting her bank concerning the possibility of fraud or identity theft following the Data breach, and exploring her options for dealing with the exposure of her Personal Information in the Data Breach.

52. Plaintiff Wilson is aware of no other source from which the theft of her Personal Information could have come. She regularly takes steps to safeguard her Personal Information in her own control.

53. Plaintiff Wilson suffered actual injury in the form of damages to and diminution of the value of her Personal Information, which she entrusted to Defendants and which was compromised in the Data Breach.

54. Plaintiff Wilson suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her Personal Information because that information was accessed and exfiltrated by hackers. This injury was exacerbated by Defendants' delay in revealing the Data Breach.

55. Following the Data Breach, Plaintiff Wilson's personal information was also discovered for sale on a dark web marketplace.

56. Plaintiff Wilson has a continuing interest in ensuring that her Personal Information, which remains with Defendants, is protected and safeguarded from future breaches.

4. Thomas Booth Harris

57. Plaintiff Thomas Booth Harris is a natural person residing in California. Plaintiff Harris is a citizen of California.

58. Plaintiff Harris has no known relationship with Defendants other than having

surgery in December 2021 under anesthesia and receiving a breach notice from Palm Springs-AS on or around October 24, 2022.

59. In order to receive healthcare services, Plaintiff Harris had to provide his Personal Information to Palm Springs-AS.

60. Plaintiff Harris did so and, upon information and belief, Palm Springs-AS passed his information along to Somnia. Plaintiff Harris trusted that Somnia and Palm Springs-AS would use reasonable measures to protect his information, including complying with state and federal law.

61. As a result of the Data Breach, Plaintiff Harris spent time dealing with the consequences of the Data Breach, including verifying the legitimacy of the breach notice, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred.

62. Plaintiff Harris has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff Harris fears for his personal financial security and uncertainty over what Personal Information was exposed in the Data Breach.

63. Plaintiff Harris has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

64. Plaintiff Harris suffered actual injury in the form of damages to and diminution in the value of his Personal Information, which was compromised in and as a result of the Data Breach.

65. Plaintiff Harris suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his Personal Information because that information was accessed and exfiltrated by hackers. This injury was exacerbated by Defendants' delay in revealing the Data Breach.

66. Plaintiff Harris has a continuing interest in ensuring that his Personal Information, which remains with Defendants, is protected and safeguarded from future breaches.

B. TEXAS

1. Irene Chabak

67. Plaintiff Irene Chabak is a natural person residing in El Paso, Texas. She is a citizen of Texas.

68. Plaintiff Chabak received anesthesia as part of a surgery at a Texas hospital in July 2022.

69. Plaintiff Chabak has no known relationship with Defendants other than having surgeries under anesthesia and receiving a breach notice from AA-El Paso on or around October 24, 2022.

70. In order to receive healthcare services, Plaintiff Chabak had to provide her Personal Information to AA-El Paso.

71. Plaintiff Chabak did so and, upon information and belief, AA-El Paso passed her information along to Somnia. Plaintiff Chabak trusted that Somnia and AA-El Paso would use reasonable measures to protect her information, including complying with state and federal law.

72. Plaintiff Chabak suffered harm as a result of the Data Breach. For example, she spent time verifying the legitimacy of the breach notice and regularly monitoring her financial accounts for any indication of fraud or identity theft.

73. Plaintiff Chabak is aware of no other source from which the theft of her Personal Information could have come. She regularly takes steps to safeguard her Personal Information in her own control.

74. Plaintiff Chabak suffered actual injury in the form of damages to and diminution of the value of her Personal Information, which she entrusted to Defendants and which was

compromised in the Data Breach.

75. Plaintiff Chabak suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her Personal Information because that information was accessed and exfiltrated by hackers. This injury was exacerbated by Defendants' delay in revealing the Data Breach.

76. Plaintiff Chabak has a continuing interest in ensuring that her Personal Information, which remains with Defendants, is protected and safeguarded from future breaches.

2. Armando Carrasco

77. Plaintiff Armando Carrasco is a natural person residing in El Paso, Texas. He is a citizen of Texas.

78. Plaintiff Carrasco received anesthesia as part of a surgery at an El Paso, Texas hospital.

79. Plaintiff Carrasco has no known relationship with Defendants other than having surgeries under anesthesia and receiving a breach notice from AA-El Paso on or around October 24, 2022.

80. In order to receive healthcare services, Plaintiff Carrasco had to provide his Personal Information to AA-El Paso.

81. Plaintiff Carrasco did so and, upon information and belief, AA-El Paso passed his information along to Somnia. Plaintiff Carrasco trusted that Somnia and AA-El Paso would use reasonable measures to protect his information, including complying with state and federal law.

82. Plaintiff Carrasco suffered harm as a result of the Data Breach. For example, he spent time exploring credit monitoring and monitoring his Experian account for signs of fraud.

83. Plaintiff Carrasco is aware of no other source from which the theft of his Personal Information could have come. He regularly takes steps to safeguard his Personal Information in

his own control.

84. Plaintiff Carrasco suffered actual injury in the form of damages to and diminution of the value of his Personal Information, which he entrusted to Defendants and which was compromised in the Data Breach.

85. Plaintiff Carrasco suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his Personal Information because that information was accessed and exfiltrated by hackers. This injury was exacerbated by Defendants' delay in revealing the Data Breach.

86. Following the Data Breach, Plaintiff Carrasco's personal information was also discovered for sale on a dark web marketplace.

87. Plaintiff Carrasco has a continuing interest in ensuring that his Personal Information, which remains with Defendants, is protected and safeguarded from future breaches.

C. ILLINOIS

1. Scott Weiscope

88. Plaintiff Scott Weiscope is a natural person residing in Mattoon, Illinois. He is a citizen of Illinois.

89. Plaintiff Weiscope received anesthesia as part of a surgery at an Illinois hospital in February 2021 and a Missouri hospital in September 2021.

90. Plaintiff Weiscope has no known relationship with Defendants other than having surgeries under anesthesia and receiving a breach notice from RAA-IL on or around October 24, 2022.

91. In order to receive healthcare services, Plaintiff Weiscope had to provide his Personal Information to RAA-IL.

92. Plaintiff Weiscope did so and, upon information and belief, RAA-IL passed his

information along to Somnia. Plaintiff Weiscope trusted that Somnia and RAA-IL would use reasonable measures to protect his information, including complying with state and federal law.

93. Plaintiff Weiscope suffered harm as a result of the Data Breach. For example, he spent time verifying the legitimacy of the breach notice and exploring his options for dealing with the exposure of his Personal Information in the Data Breach.

94. Plaintiff Weiscope is aware of no other source from which the theft of his Personal Information could have come. He regularly takes steps to safeguard his Personal Information in his own control.

95. Plaintiff Weiscope suffered actual injury in the form of damages to and diminution of the value of his Personal Information, which he entrusted to Defendants and which was compromised in the Data Breach.

96. Plaintiff Weiscope suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his Personal Information because that information was accessed and exfiltrated by hackers. This injury was exacerbated by Defendants' delay in revealing the Data Breach.

97. Following the Data Breach, Plaintiff Weiscope's personal information was also discovered for sale on a dark web marketplace and in January 2023, Credit Karma alerted Plaintiff Weiscope that his Personal Information had been located on the dark web.

98. Plaintiff Weiscope has a continuing interest in ensuring that his Personal Information, which remains with Defendants, is protected and safeguarded from future breaches.

D. NEW MEXICO

1. Lavina Henderson

99. Plaintiff Lavina Henderson is a natural person residing in Farmington, New Mexico. She is a citizen of New Mexico.

100. On or around October 24, 2022, Ms. Henderson received a breach notice from RAA-NM.

101. In order to receive healthcare services, Ms. Henderson had to provide her Personal Information to RAA-NM.

102. Ms. Henderson did so and, upon information and belief, RAA-NM passed her information along to Somnia. Ms. Henderson trusted that Somnia and RAA-NM would use reasonable measures to protect her information, including complying with state and federal law.

103. Ms. Henderson is very careful about sharing her sensitive Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. She stores any documents containing her Private Information in a safe and secure location or destroys the documents.

104. As a result of the Data Breach, Ms. Henderson has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the breach notice, exploring credit monitoring and identity theft protection services, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred.

105. Ms. Henderson suffered actual injury in the form of damages to and diminution in the value of her Private Information, which was compromised in and as a result of the Data Breach.

106. Ms. Henderson has suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

107. Ms. Henderson suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her Personal Information because that information was accessed and exfiltrated by hackers. This injury was exacerbated by Defendants' delay in revealing the Data Breach.

108. Ms. Henderson has a continuing interest to ensure that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

2. Jeremy Henderson

109. Plaintiff Jeremy Henderson is a natural person residing in Farmington, New Mexico. He is a citizen of New Mexico.

110. On or around October 24, 2022, Mr. Henderson received a breach notice from RAA-NM.

111. In order to receive healthcare services, Mr. Henderson had to provide his Personal Information to RAA-NM.

112. Mr. Henderson did so and, upon information and belief, RAA-NM passed his information along to Somnia. Mr. Henderson trusted that Somnia and RAA-NM would use reasonable measures to protect his information, including complying with state and federal law.

113. Mr. Henderson is very careful about sharing his sensitive Private Information. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. He stores any documents containing his Private Information in a safe and secure location or destroys the documents.

114. As a result of the Data Breach, Mr. Henderson has spent time dealing with the consequences of the Data Breach, which include time spent verifying the legitimacy of the breach notice, exploring credit monitoring and identity theft protection services, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred.

115. Mr. Henderson suffered actual injury in the form of damages to and diminution in the value of his Private Information, which was compromised in and as a result of the Data Breach.

116. Mr. Henderson has suffered lost time, annoyance, interference, and inconvenience

because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

117. Mr. Henderson suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his Personal Information because that information was accessed and exfiltrated by hackers. This injury was exacerbated by Defendants' delay in revealing the Data Breach.

118. Following the Data Breach, Mr. Henderson's personal information was also discovered for sale on a dark web marketplace.

119. Mr. Henderson has a continuing interest to ensure that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

IV. DEFENDANTS

A. SOMNIA, INC.

120. Defendant Somnia, Inc. is a New York corporation with its principal place of business in Harrison, New York.

B. ANESTHESIA SERVICES OF SAN JOAQUIN, P.C.

121. Defendant AS-San Joaquin is a California corporation with its business address in Harrison, New York.

C. PALM SPRINGS ANESTHESIA SERVICES, P.C.

122. Defendant Palm Springs-AS is a California corporation with its business address in Harrison, New York.

D. RESOURCE ANESTHESIOLOGY ASSOCIATES OF IL, P.C.

123. Defendant RAA-IL is an Illinois corporation with its business address in Harrison, New York.

E. RESOURCE ANESTHESIOLOGY ASSOCIATES OF NM INC.

124. Defendant RAA-NM is a New Mexico corporation with its business address in New Rochelle, New York.

F. ANESTHESIA ASSOCIATES OF EL PASO, P.A.

125. Defendant AA-El Paso is a Texas corporation with its business address in Harrison, New York.

V. FACTUAL ALLEGATIONS

A. DEFENDANTS' COLLECTION OF PERSONAL INFORMATION.

126. Somnia is an anesthesiology services provider and practice management company that owns and manages numerous anesthesiology practices across the United States. Its website states that its vision is “to be the smartest choice in anesthesia practice management for healthcare facilities across the country.”³

127. Per the National Provider Identifier database, Dr. Marc E. Koch is identified as the authorized President and CEO of Somnia, as well as AS-San Joaquin, Palm Springs-AS, and RAA-NM. All Defendants except RAA-NM share a registered mailing address in Harrison, New York.

128. The anesthesiology practices that Somnia works with obtain Class Members' Personal Information when patients receive anesthesiology. This includes, but is not limited to:

- a. Contact information;
- b. Authentication information, such as driver's licenses and Social Security Numbers;
- c. Demographic information;
- d. Payment information; and

³ Somnia, Our Mission, <https://somniaanesthesiaservices.com/somnia-anesthesia/company-mission/> (last accessed Feb. 22, 2023).

e. Medical history as reported by patients and other healthcare providers.

129. Obtaining this information is a precondition of receiving anesthesiology services.

130. Defendants AS-San Joaquin, Palm Springs-AS, AA-El Paso, RAA-IL, and RAA-NM collect and maintain patient and former patient Personal Information. This information subsequently is transferred to Somnia.

B. THE DATA BREACH.

131. On July 11, 2022, Somnia belatedly discovered “suspicious activity on its systems.”⁴ While Somnia did not disclose what led it to this discovery or what the suspicious activity was, its notices indicated that its attempted remediation required it to “disconnect[] all systems” and to undertake a “global password change,” “tighten[] firewall restrictions, and deploy[] endpoint threat detection and response monitoring software on workstations and servers.”⁵ The impacted information involved includes “names, and some combination of the following data elements: Social Security number, date of birth, driver’s license number, financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis info.”⁶ It also included “a limited amount of personal information for some Somnia employees.”⁷

132. The need to tighten firewall restrictions indicates that the hackers were able to install malware that provided them with a “backdoor” into Somnia’s system wherein they could roam freely without detection throughout Somnia’s systems. This demonstrates that there was a total breach of Somnia’s systems.

⁴ Somnia, Security Incident, <https://somniaanesthesiaservices.com/somnia-anesthesia/security-incident/> (last accessed Mar. 1, 2023).

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

133. Further, the need to deploy endpoint threat detection demonstrates that either Somnia: (1) did not have antivirus software installed on its servers and workstations (in violation of every basic security requirement) or (2) its patchwork antivirus software failed to detect the hackers. Either way, having effective antivirus software is a basic security precaution that any company must employ, particularly one such as Somnia that holds patients' PHI.

134. The result of Somnia's investigation was stark. The investigation revealed that the information detailed above may have been compromised. Somnia offered "credit monitoring and identity protection services" and stated that it "deeply regret[s] any concern this has caused our partners and patient community."⁸

135. On September 22, 2022, Somnia informed the Defendant Anesthesiology Providers of the Data Breach and stated on its website that it provided notice to "impacted individuals on September 22 and 23, 2022, through substitute notice."⁹

136. On October 24, 2022, additional notice was sent to Plaintiffs and Class Members from their specific anesthesiology providers, including the Defendant Anesthesiology Providers. This notice provided the scant details above and offered identity theft protection services to recipients.

137. The information provided to the U.S. Department of Health and Human Services Office for Civil Rights Data Breach Portal listed the "location of breached information" as "network server," but otherwise did not contain additional information about the cause of the breach.¹⁰

⁸ *Id.*

⁹ *Id.*

¹⁰ U.S. Dep't of Health & Human Servs. Office for Civil Rights, Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Mar. 1, 2023).

C. DEFENDANTS' NOTICE WAS DEFICIENT.

138. Defendants' notices concerning the Data Breach were deficient both in their content and their unexplained tardiness.

139. Defendants' notices, which were substantively identical, do not provide critical information: how long the unauthorized attackers were inside of Somnia's systems, how unauthorized attackers were able to get inside Somnia's systems without detection, and how unauthorized attackers were able to exfiltrate Personal Information without detection.

140. Defendants' notices do not explain precisely what Personal Information was taken, stating broadly that "information stored in the Management Company's system could include some combination of patient names, addresses, health insurance policy number, Social Security numbers, payment information, and health information such as treatment and diagnosis."¹¹

141. Furthermore, Defendants' notices failed to explain the extent to which the unauthorized attackers were able to compromise Somnia's systems. The notices vaguely state that the Defendant Anesthesiology Providers were informed by Somnia of "suspicious activity."¹² In what way the activity was "suspicious" or how the activity was "identified" remains unexplained.

142. The notice is also silent as to whether Plaintiffs and Class Members' information is still being stored with Somnia. In fact, the notices do not even name Somnia, referring to it instead as a "management company."¹³

143. Numerous state laws required Defendants to provide prompt notice of the Data Breach. Defendants failed to do so. Somnia stated that the Data Breach was discovered on July 11,

¹¹ See, e.g., *Sommers v. Somnia, Inc.*, Case No. 7:22-cv-10572-PMH (S.D.N.Y.), Dkt. 1-1 (Notice of Data Breach Ltr. from AS-San Joaquin to Plaintiff Sommers).

¹² *Id.* at 1.

¹³ *Id.*

2022. However, it was not until September 21 and 22, 2022 that Somnia even informed its contractual partners, including the Defendant Anesthesiology Providers, of the Data Breach.

144. Somnia did not provide any notice until September 22 and 23, 2022, in what it describes on its website as “substitute notice.”¹⁴ What actions it took are unclear.

145. It was not until October 24, 2022, that the Defendant Anesthesiology Providers mailed letters to “impacted individuals.” At that point, three months had passed; Plaintiffs and Class Members were left wondering what of their information was taken. This delay also left Plaintiffs and Class Members at least three months behind the unauthorized attackers who exfiltrated their Personal Information. Somnia informed the U.S. Department of Health and Human Services Office for Civil Rights Data Breach Portal that same day and placed the same vague language on its website.¹⁵

146. Plaintiffs and Class Members are left trying to understand what happened with their Personal Information, what risks they face, and the period during which their Personal Information was improperly taken.

D. DEFENDANTS FAILED TO SAFEGUARD PERSONAL INFORMATION.

147. Defendants failed to exercise reasonable care in protecting patients’ information.

148. Defendants have a non-delegable duty under federal law to ensure that all information they collect, and store is secure, and that any associated entities with whom they shared information maintain adequate and commercially reasonable data security practices to ensure the protection of patients’ Personal Information.

149. Indeed, Defendants’ entire business depends on patients entrusting them with their

¹⁴ Somnia, Security Incident, <https://somniaanesthesiaservices.com/somnia-anesthesia/security-incident/> (last accessed Mar. 1, 2023).

¹⁵ *Id.*

Personal Information. Without patients' Personal Information, Defendants would not be able to perform any services and certainly would not be able to bill patients and their insurance companies and collect payment for services rendered.

150. More specifically, to provide services to patients, the Defendant Anesthesiology Providers know that their patients must trust that they are keeping their health information private and secure. If those patients lack trust in them or know they insecurely store, safeguard, or transmit their personal information, then they will not disclose health information to them and will choose a different provider for services.

151. Defendants are entities covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), *see* 45 C.F.R. § 160.102, and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

152. These rules establish national standards for the protection of patient information, including "protected health information," defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

153. HIPAA limits the permissible uses of "protected health information," prohibits unauthorized disclosures of "protected health information," and requires that Defendants implement appropriate safeguards for this information.

154. Under HIPAA, covered entities such as Defendants may only disclose PHI to a “business associate” if the covered entity obtains satisfactory assurances that the business associate, here Somnia, will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.¹⁶

155. HIPAA further mandates that Defendants disclose no more PHI to a business associate than what is minimally necessary to accomplish the purposes for which it was engaged by the covered entity. 45 C.F.R § 164.502(b).

156. HIPAA requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons (i.e. unencrypted data).

157. Somnia’s website asserts, “Somnia, Inc. and its affiliates (collectively referred to as ‘Somnia’) are committed to fulfilling their obligations under Health Insurance Portability and Accountability Act (HIPAA) and to safeguarding the protected health information (PHI) of patients.”¹⁷

158. Somnia’s Corporate Brochure further assures, “We adhere to HIPAA guidelines, utilizing a read-only virtual private network to protect the exchange of patient information and reduce the shortcomings of paper-based transmittals.”¹⁸

159. Somnia’s vague notices indicate that it failed to detect unauthorized attackers, had

¹⁶ See 45 CFR §§ 164.502(e), 164.504(e), 164.532(d) and (e).

¹⁷ Somnia, Legal, <https://somniaanesthesiaservices.com/legal/> (last accessed Mar. 1, 2023).

¹⁸ Somnia, *Corporate Brochure*, at 8

https://f.hubspotusercontent10.net/hubfs/49769/docs/Somnia_BD_Brochure_pages_Jan2016.pdf (last accessed Mar. 1, 2023).

information exfiltrated without detection, and that its security was so deficient that it required a “global password change, tightening firewall restrictions, and [the deployment of] endpoint threat detection and response monitoring software on workstations and servers.”¹⁹

160. As detailed above, these remediation measures plausibly demonstrate that hackers were able to totally compromise Somnia’s systems by installing malware that Somnia’s antivirus software, to the extent it existed, failed to detect.

161. The unstated length of time between the Data Breach and Somnia’s claimed discovery of the Data Breach indicates that Somnia’s systems to detect intrusion, detect unusual activity, and log and report such events were inadequate and not in compliance with industry standards. For example, according to technology security company FireEye, the median amount of time between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been trending downward in recent years due to improvements in detection computer technology.²⁰ The fact that Somnia did not even disclose how long it took to detect the Data Breach is direct evidence of its failure to employ reasonable, industry-standard data security practices to safeguard Plaintiffs’ and Class Members’ Personal Information.

E. DEFENDANTS VIOLATED REGULATORY GUIDANCE AND HIPAA’S REQUIREMENTS TO SAFEGUARD DATA.

162. Defendants failed to maintain the privacy and security of their patients’ PHI and failed to inform patients that their Personal Information was disclosed. Indeed, Defendants violated HIPAA by failing to:

¹⁹ Somnia, Security Incident, <https://somniaanesthesiaservices.com/somnia-anesthesia/security-incident/> (last accessed Mar. 1, 2023).

²⁰ *M-Trends 2019: FireEye Mandiant Services Special Report*, <https://content.fireeye.com/m-trends/rpt-m-trends-2019> (last accessed Feb. 22, 2023).

- a. Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Adequately protect Plaintiffs' and Class Members' Personal Information;
- c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);
- e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);
- f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);
- h. Take safeguards to ensure that Defendants' business associates adequately store protected health information;
- i. Disclose only PHI necessary for Defendants' business associates to accomplish the purposes for which they were engaged, in violation of 45 C.F.R. § 164.502(b); and

j. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4).

163. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission (“FTC”) has issued numerous guides for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.²¹

164. The FTC’s *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow to protect sensitive data. Among other things, it notes that businesses should: (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network’s vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large volumes of data being transmitted from their system, and have a response plan ready in the event of a breach.²²

165. Additionally, the FTC recommends that organizations limit access to sensitive data, require the use of complex passwords on networks, employ industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.²³

²¹ FTC, *Start With Security: A Guide for Businesses*, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed Feb. 22, 2023).

²² *Id.*

²³ *Id.*

166. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.²⁴

167. Defendants were fully aware of their obligations to implement and use reasonable measures to protect the Personal Information of Plaintiffs and Class Members, but failed to comply with these basic recommendations and guidelines that would have prevented the Data Breach from occurring.

F. PLAINTIFFS' AND CLASS MEMBERS' PERSONAL INFORMATION IS HIGHLY VALUABLE.

168. Defendants were or should have been aware that they were collecting highly valuable data, which has increasingly been the target of data breaches in recent years.²⁵

169. The U.S. Department of Health and Human Services, Office for Civil Rights, lists the Data Breach as one of the largest healthcare breaches reported in 2022.²⁶

170. As early as 2014, the FBI alerted the healthcare industry that it was increasingly a preferred target of hackers, stating “[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or

²⁴ FTC, *Privacy and Security Enforcement*, <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last accessed Feb. 22, 2023).

²⁵ Healthcare Data Breach Statistics, HIPAA Journal, <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (last accessed Feb. 22, 2023) (“Our healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 10 years.”).

²⁶ U.S. Dep’t of Health and Human Services, Office for Civil Rights, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Feb. 22, 2023).

Personally Identifiable Information (PII)” so that these companies could take the necessary precautions to thwart such attacks.²⁷

171. Further, Cathy Allen, CEO of Shared Assessments, a cyber-risk management group, stated that “just the types of test proscribed might indicate a type of illness that you would not want employers or insurance companies to have. Thieves often steal and resell insurance data on the internet . . . having other information makes the data more valuable and the price higher.”²⁸

172. Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the “cyber black-market.” As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security numbers, and other Personal Information on the dark web, making the information publicly available.²⁹

173. Healthcare data is especially valuable on the black market. According to one report, a healthcare data record may be valued at up to \$250 per record, compared to \$5.40 for the next highest value record (a payment card).³⁰

174. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on the

²⁷ Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS, Aug. 20, 2014, <http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820> (last accessed Feb. 22, 2023).

²⁸ *Id.*

²⁹ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Feb. 22, 2023); McFarland et al., *The Hidden Data Economy*, at 3, <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf> (last accessed Feb. 22, 2023).

³⁰ *Hackers, Breaches, and the Value of Healthcare Data* (June 20, 2021), <https://www.securelink.com/blog/healthcare-data-new-prize-hackers/> (last accessed Feb. 22, 2023).

black market “includes names, birth dates, policy numbers, diagnosis codes and billing information.”³¹ Fraudsters commonly use that data “to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers.”³²

175. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, “[h]ealth information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an individual.”³³ For this reason, a patient’s full medical records can sell for up to \$1,000 on the dark web, while credit card numbers and Social Security numbers may cost \$5 or less.³⁴

176. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies:

The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient’s medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient’s identity to open credit cards and fraudulent loans.³⁵

³¹ Jim Finkle, *Your medical record is worth more to hackers than your credit card*, Reuters, <https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924> (last accessed Feb. 22, 2023).

³² *Id.*

³³ Andrew Steger, *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (last accessed Feb. 22, 2023).

³⁴ Paul Nadrag, *Here’s How Much Your Personal Information Is Selling for on the Dark Web* (Dec. 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Feb. 22, 2023).

³⁵ *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web* (Jan. 26, 2021), <https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web> (last visited Feb. 22, 2023).

G. DEFENDANTS HARMED PLAINTIFFS AND CLASS MEMBERS BY ALLOWING ANYONE TO ACCESS THEIR PERSONAL INFORMATION.

177. Defendants knew or should have known both that medical information is incredibly valuable to hackers and that health care data breaches are on the rise. Accordingly, Defendants were on notice for the harms that could ensue if they failed to protect patients' data.

178. Given the sensitive nature of the Personal Information stolen in the Data Breach—including Social Security numbers, dates of birth, driver's license numbers, financial account information, health insurance policy numbers, Medical Record Numbers, Medicaid or Medicare IDs, and health information, such as treatment and diagnosis info—hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and in the indefinite future.

179. Almost immediately after the Data Breach, Class Members' Personal Information was for sale on the dark web.

180. Plaintiffs and Class Members have already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

181. The Personal Information exposed in the Data Breach is highly coveted and valuable on underground or black markets—and information tied to this Data Breach has already been offered for sale.

182. Identity thieves can use the stolen information to: (a) create fake credit cards that are used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, extortion, and other negative effects.

183. While federal law generally limits an individual's liability for fraudulent credit card charges to \$50, there are no such protections for a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of \$13,500 in out-of-pocket costs to resolve the crime.³⁶ Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%).

184. According to the Ponemon study, “[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate.”³⁷

³⁶ Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 (last accessed Feb. 22, 2023).

³⁷ *Id.* at 2.

185. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.³⁸

186. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the resolution of the crime.³⁹ In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."⁴⁰

187. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits;
- Receive information from their health plan that they have reached their limit on benefits; or

³⁸ *Id.* at 14.

³⁹ *Id.* at 1.

⁴⁰ *Id.*

- Are denied insurance because their medical records show a condition they do not have.⁴¹

188. Other types of medical fraud include “leveraging details specific to a disease or terminal illness, and long-term identity theft.”⁴² According to Tom Kellermann, “[t]raditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do.”⁴³ Long-term identity theft occurs when fraudsters combine a victim’s data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

189. As explained further by the FTC, medical identity theft can have other serious consequences:

Medical ID thieves may use your identity to get treatment – even surgery – or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person’s health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer’s unpaid medical debts also could end up on your credit report.⁴⁴

190. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm

⁴¹ FTC, *Medical Identity Theft FAQs for Health Care Providers and Health Plans*, <https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf> (last accessed Feb. 22, 2023).

⁴² Steger, *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (last accessed Feb. 22, 2023).

⁴³ *Id.*

⁴⁴ *Medical ID Theft: Health Information for Older People*, Federal Trade Commission, <https://web.archive.org/web/20201019075254/https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people> (last accessed Feb. 22, 2023).

for which they are entitled to damages, including, but not limited to, the following:

- a. losing the inherent value of their Personal Information;
- b. identity theft and fraud resulting from the theft of their Personal Information;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;
- e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- f. lowered credit scores resulting from credit inquiries following fraudulent activities;
- g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts; and
- h. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

191. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.⁴⁵

192. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendants would have no reason to tout their data security efforts to their actual and potential customers.

193. Consequently, had consumers known the truth about Defendants' data security practices—that they did not adequately protect and store their Personal Information—they would not have entrusted their Personal Information to Defendants.

H. HACKERS SOLD CLASS MEMBERS' PERSONAL INFORMATION ON THE DARK WEB.

194. Following the Data Breach, there is evidence that the exfiltrated Personal Information was available for purchase on the dark web.

195. Specifically, Plaintiffs' consulting expert searched for and found evidence as early as July 21, 2022, days after Somnia discovered the Data Breach, that access to stolen Somnia information was available for sale on the dark web.

196. This information was available for sale prior to the Data Breach being publicly announced.

⁴⁵ FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), <https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf> (last visited Feb. 22, 2023).

197. Further, it appears that the seller is associated with a known malware service notorious for stealing data.

198. As detailed below, the consulting expert also searched for Plaintiffs' Personal Information on the dark web and there was evidence for such information for several Plaintiffs.

CLASS ACTION ALLEGATIONS

A. CLASS DEFINITIONS

1. NATIONWIDE CLASS

199. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

All natural persons residing in the United States whose Personal Information was compromised in the Data Breach.

200. The Nationwide Class asserts claims against each Defendant for negligence (Count 1), negligence *per se* (Count 2), breach of confidence (Count 3), and unjust enrichment (Count 4).

2. THE DEFENDANT ANESTHESIOLOGY PROVIDER-SPECIFIC SUBCLASSES

201. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of Defendant-specific claims on behalf of those individuals who provided their information to each specific Defendant Anesthesiology Provider (the "Defendant Anesthesiology Provider Subclasses"), defined as follows:

All natural persons residing in the United States whose Personal Information was compromised in the Data Breach, and who obtained services from [name of Defendant Anesthesiology Provider].

202. Each Defendant Anesthesiology Provider-Specific Subclass will be represented by the Plaintiff(s) who provided their information to each Defendant Anesthesiology Provider. Specifically, (1) Plaintiff Sommers will represent the AS-San Joaquin Subclass; (2) Plaintiffs Polk, Wilson, and Harris will represent the Palm Springs-AS Subclass; (3) Plaintiff Weiscope will

represent the RAA-IL Subclass; (4) Plaintiffs Lavina Henderson and Jeremy Henderson will represent the RAA-NM Subclass; and (5) Plaintiffs Chabak and Carrasco will represent the AA-El Paso Subclass.

3. STATEWIDE SUBCLASSES

203. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claim in the alternative to the nationwide claims, as well as statutory claims under California data breach statutes and consumer protection statutes (Counts 5 through 8), on behalf of separate statewide subclasses for each State (the “Statewide Subclasses”), defined as follows:

All natural persons residing in [name of state] whose Personal Information was compromised in the Data Breach.

204. Excluded from the Class are Defendants, any entity in which any Defendant has a controlling interest, and any Defendants’ officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

205. Plaintiffs reserve the right to modify or amend the definitions of the Class before the Court determines whether certification is appropriate.

B. THE PROPOSED CLASSES MEET THE RELEVANT RULE 23 REQUIREMENTS.

206. **Numerosity. Federal Rule of Civil Procedure 23(a)(1).** The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, Defendants have acknowledged that hundreds of thousands of their customers’ Personal Information has been compromised. Those individuals’ names and addresses are available from Defendants’ records, and Class Members may be notified of the pendency of

this action by recognized, Court-approved notice dissemination methods. There are at least thousands of Class Members in each State Subclass, making joinder of all State Subclass members impracticable.

207. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

- a. Whether Defendants had a duty to protect Personal Information;
- b. Whether Defendants failed to take reasonable and prudent security measures;
- c. Whether the Defendant Anesthesiology Providers knew or should have known of the susceptibility of Somnia's systems to a data breach;
- d. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;
- e. Whether Defendants' security measures to protect their systems were reasonable in light known legal requirements;
- f. Whether Defendants' efforts (or lack thereof) to ensure the security of patients' Personal Information were reasonable in light of known legal requirements;
- g. Whether Defendants' conduct constituted unfair or deceptive trade practices;
- h. Whether Defendants violated state law when they failed to implement reasonable security procedures and practices;

- i. Which security procedures and notification procedures Defendants should be required to implement;
- j. Whether Defendants violated state consumer protection and data breach statutes in connection with the actions described herein;
- k. Whether Defendants failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the data breach was discovered;
- l. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach and/or the loss of the Personal Information of Plaintiffs and Class Members;
- m. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect their Personal Information; and
- n. Whether Plaintiffs and Class Members are entitled to damages or injunctive relief.

208. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' Personal Information was in Defendants' possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

209. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are an adequate representative of the Class because Plaintiffs are a member of the Class and are committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in

litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

210. Predominance & Superiority. Fed. R. Civ. P. 23(b)(3). Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

211. Risk of Prosecuting Separate Actions. This case is appropriate for certification because prosecuting separate actions by individual Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Defendants or would be dispositive of the interests of members of the Class.

212. **Ascertainability.** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. The Class and Subclasses consist of individuals who received services from the Defendant Anesthesiology Providers and whose information was supplied to Somnia. Class membership can be determined using Defendants' records, presumably also how Defendants were able to provide notice of breach letters to Plaintiffs and Class Members.

213. **Injunctive Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect Class Members' data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

214. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;
- b. Whether Defendants failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class Members;
- c. Whether the Defendant Anesthesiology Providers failed to adequately monitor and audit the data security systems of Somnia;
- d. Whether Defendants were unfairly and unjustly enriched as a result of their improper conduct, such that it would be inequitable for Defendants to retain the benefits conferred

upon them by Plaintiffs and the other Class Members; and

e. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

**On Behalf of Plaintiffs against Somnia
and on behalf of each Defendant Anesthesiology Provider-Specific Subclass Representative
against each applicable Defendant Anesthesiology Provider**

215. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

216. Defendants required Plaintiffs and Class Members to submit Personal Information to anesthesiology providers, including the Defendant Anesthesiology Providers; Somnia subsequently received the Personal Information from the providers. Defendants collected and stored the Personal Information for commercial gain.

217. Defendants knew or should have known that Somnia's systems were vulnerable to unauthorized access and exfiltration by third parties.

218. Defendants had a non-delegable duty to maintain adequate and commercially reasonable data security practices to ensure the protection of patients' Personal Information.

219. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' Personal Information within their control from being compromised, lost, stolen, accessed, or misused by unauthorized persons.

220. Defendants owed a duty of care to Plaintiffs and Class Members to provide security,

consistent with industry standards, to ensure that the systems and networks Defendants utilized adequately protected their Personal Information.

221. Defendants' duty to use reasonable security measures arose from the special relationship that existed between Defendants and the Plaintiffs and Class Members. The special relationship arose because Plaintiffs and Class Members entrusted Defendants with their Personal Information as part of their healthcare services. Only Defendants were in a position to ensure that they had sufficient safeguards to protect against the harm to Plaintiffs and Class Members that would result from a data breach.

222. Defendants' duty to use reasonable care in protecting Personal Information arose from the common law and the statutes and regulations, as well as their own promises regarding privacy and data security to patients. This duty exists because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining the personal and confidential information of Plaintiffs and Class Members and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendants did not protect Plaintiffs' and Class Members' Personal Information from hackers.

223. Defendants' duties also arose under HIPPA regulations, which, as described above, apply to Defendants and establish national standards for the protection of patient information, including protected health information, which require Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA further mandates that Defendants disclose no more PHI to a business associate than what is minimally necessary to accomplish the purposes

for which the business associate was engaged. 45 C.F.R § 164.502(b). The confidential data at issue in this case constitutes “protected health information” within the meaning of HIPAA.

224. Defendants’ duties also arose under Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further establish Defendants’ duty. In addition, several individual states have enacted statutes based upon the FTC Act that also create a duty.

225. Defendants knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of their systems, and the importance of adequate security.

226. Defendants breached their common law, statutory, and other duties—and thus were negligent—by failing to use reasonable measures to protect patients’ Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

227. Defendants breached their duties to Plaintiffs and Class Members in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs’ and Class Members’ Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

- d. Failing to adequately monitor, evaluate, and ensure the security of Somnia's network and systems;
- e. Failing to disclose to Somnia only PHI that was necessary to accomplish the purposes for which Somnia was engaged;
- f. Failing to recognize in a timely manner that Plaintiffs' and other Class Members' Personal Information had been compromised; and
- g. Failing to timely and adequately disclose that Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed.

228. Plaintiffs' and Class Members' Personal Information would not have been compromised but for Defendants' wrongful and negligent breach of their duties.

229. Defendants' failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' Personal Information.

230. It was also foreseeable that Defendants' failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members as described in this Complaint.

231. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information.

232. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members suffered damages and will suffer damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiffs and Class Members; damages

arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take years to discover and detect; and loss of the value of their privacy and confidentiality of the stolen confidential data, including health data.

COUNT 2

NEGLIGENCE PER SE

**On Behalf of Plaintiffs against Somnia
and on behalf of each Defendant Anesthesiology Provider-Specific Subclass Representative
against each applicable Defendant Anesthesiology Provider**

233. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

234. Defendants are entities covered by HIPAA, 45 C.F.R. § 160.102, and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

235. HIPAA requires Defendants to “reasonably protect” confidential data from “any intentional or unintentional use or disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1). HIPAA also requires medical service providers, such as Defendant Anesthesiology Providers, to obtain satisfactory assurances that their business associates, such as Somnia, would appropriately safeguard the protected health information it receives or creates on

behalf of the Defendants. 45 CFR § 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes “protected health information” within the meaning of HIPAA. Somnia constitutes a “business associate” within the meaning of HIPAA.

236. HIPAA further requires Defendants to disclose the unauthorized access and theft of the Personal Information to Plaintiffs and Class Members “without unreasonable delay” so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, 406, & 410.

237. Defendants violated HIPAA by failing to reasonably protect Plaintiffs’ and Class Members’ Personal Information, as described herein.

238. Defendants’ violations of HIPAA constitute negligence *per se*.

239. Plaintiffs and Class Members are within the class of persons that HIPAA was intended to protect.

240. The harm that occurred due to the Data Breach is the type of harm against which HIPAA was intended to guard.

241. Additionally, Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

242. The FTC publications and orders described above also form part of the basis of Defendants’ duty in this regard.

243. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendants’

conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as Somnia, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

244. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

245. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

246. The harm that occurred due to the Data Breach is the type of harm against which the FTC Act was intended to guard. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm Plaintiffs and Class Members have suffered.

247. As a direct and proximate result of Defendants' negligence per se under HIPAA and the FTC Act, Plaintiffs and Class Members have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT 3

BREACH OF CONFIDENCE

**On Behalf of Plaintiffs against Somnia
and on behalf of each Defendant Anesthesiology Provider-Specific Subclass Representative
against each applicable Defendant Anesthesiology Provider**

248. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

249. Plaintiffs and Class Members maintained a confidential relationship with Defendants whereby Defendants undertook a duty not to disclose the Personal Information provided by Plaintiffs and Class Members to Defendants to any unauthorized third party or parties. Such Personal Information was confidential and novel, highly personal and sensitive, and not

generally known.

250. Defendants knew Plaintiffs' and Class Members' Personal Information was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the Personal Information they collected, stored, and maintained.

251. Defendants required Plaintiffs and Class Members to provide their Personal Information to them in order to receive medical treatment.

252. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' Personal Information in intentional, knowing, and/or negligent breach of this duty. The unauthorized disclosure occurred because Defendants failed to implement and maintain reasonable safeguards to protect the Personal Information in their possession and failed to comply with industry-standard data security practices.

253. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to unauthorized third parties.

254. As a direct and proximate result of Defendants' breach of confidence, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT 4

UNJUST ENRICHMENT **On Behalf of Plaintiffs against Somnia** **and on behalf of each Defendant Anesthesiology Provider-Specific Subclass Representative** **against each applicable Defendant Anesthesiology Provider**

255. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

256. For years and continuing to today, Defendants' business models depended upon

patients entrusting them with their Personal Information. Trust and confidence are critical and central to both the services provided by Defendants to patients, and the billing and collection for such services. Unbeknownst to Plaintiffs and Class Members, however, Defendants failed to reasonably or adequately secure, safeguard, and otherwise protect Plaintiffs' and Class Members' Personal Information. Defendants' deficiencies described herein were contrary to the information they provided to Plaintiffs and Class Members.

257. Plaintiffs and Class Members engaged Defendants for services and provided Defendants with, and allowed Defendants to collect, their Personal Information on the mistaken belief that Defendants complied with their duty to safeguard and protect patients' Personal Information. Defendants knew that the manner in which they maintained and transmitted patients' Personal Information violated their fundamental duties to Plaintiffs and Class Members by disregarding industry-standard security protocols to ensure confidential information was securely transmitted and stored.

258. Defendants had within their exclusive knowledge at all relevant times the fact that they had failed to implement adequate security measures to keep patients' Personal Information secure. This information was not available to Plaintiffs, Class Members, or the public at large.

259. Defendants also knew that Plaintiffs and Class Members expected that their information would be kept secure against known security risks and that Defendants' business associates would be vetted before they received patients' Personal Information. And based on this expectation and trust, Defendants knew that Plaintiffs and Class Members would not have disclosed health information to them and would have chosen different service providers if Plaintiffs and Class Members knew those expectations were not met.

260. Plaintiffs and Class Members did not expect that Defendants would store or

transmit their Personal Information insecurely.

261. Had Plaintiffs and Class Members known of Defendants' deficient security practices, Plaintiffs and Class Members would not have engaged Defendants to perform any services and would never have provided Defendants with their Personal Information.

262. By withholding these material facts, Defendants put their own interests ahead of their patients' interests and benefitted themselves to the detriment of Plaintiffs and Class Members.

263. As a result of their conduct as alleged herein, Defendants sold more services than they otherwise would have and were able to charge Plaintiffs and Class Members when they otherwise could not have. Defendants were unjustly enriched by charging and collecting for those services to the detriment of Plaintiffs and Class Members.

264. To be sure, this is not a question of whether Defendants misused patients' Personal Information. It is more foundational. Defendants promised to protect and safeguard Plaintiffs' and Class Members' Personal Information at all times (from the inception of their relationship of trust and confidence) and never would have performed any services of value enabling them to bill or collect payment but for Defendants' unfair and deceptive practices.

265. It would be inequitable, unfair, and unjust for Defendants to retain these wrongfully obtained benefits. Defendants' retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

266. Defendants' defective security and their unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their private Personal Information.

267. Each Plaintiff and Class Member is entitled to restitution and non-restitutionary disgorgement in the amount by which Defendants were unjustly enriched, to be determined at trial.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 5

CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT

Cal. Civ. Code §§ 56, et seq.

**On Behalf of California Plaintiffs against Somnia
and on behalf of each Defendant Anesthesiology Provider-Specific Subclass Representative
against each applicable Defendant Anesthesiology Provider**

268. The California Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

269. California’s Confidentiality of Medical Information Act (“CMIA”) requires a healthcare provider “who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein.” Cal. Civ. Code § 56.101. “Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.” *Id.*

270. The CMIA further requires that “[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information.” Cal. Civ. Code § 56.101(b)(1)(A).

271. Plaintiffs and California Subclass members are “patient[s],” “whether or not still living, who received health care services from a provider of health care and to whom medical information pertains” pursuant to § 56.05(j) of the CMIA.

272. Defendants are each a “provider of healthcare” pursuant to § 56.05(m) of the CMIA “who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information.”

273. Defendants are subject to the requirements and mandates of the CMIA and are therefore required to do the following under the CMIA:

- a. Ensure that medical information regarding patients is not disclosed or disseminated or released without patients' authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Cal. Civ. Code §§ 56.06, 56.10, 56.13, 56.245, 56.26, 56.35, 56.36, and 56.101;
- b. Not disclose medical information regarding a patient without first obtaining an authorization under Cal. Civ. Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, and 56.35;
- c. Create, maintain, preserve, and store medical records in a manner that preserves the confidentiality of the information contained therein under Cal. Civ. Code §§ 56.06 and 56.101(a);
- d. Protect and preserve confidentiality of electronic medical information in their possession under Cal. Civ. Code §§ 56.06 and 56.101(b)(1)(A); and
- e. Take appropriate preventive actions to protect confidential information or records from unauthorized release under Cal. Civ. Code § 56.36I(2)(E).

274. The Personal Information of Plaintiffs and California Subclass members compromised in the Data Breach constitutes "medical information" maintained in electronic form pursuant to § 56.05(j) of the CMIA.

275. The medical information compromised included Plaintiffs' and California Subclass members' full names, dates of birth, Social Security numbers, driver's license information and genders, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis information.

276. Due to Defendants' negligent creation, maintenance, preservation, and/or storage of Plaintiffs' and California Subclass members' electronic medical information, Defendants allowed Plaintiffs' and California Subclass members' individually identifiable medical information to be accessed and actually viewed by at least one unauthorized third party, constituting a release in violation of Cal. Civ. Code § 56.101(b)(1)(A).

277. Defendants disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(i), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). Plaintiffs and California Subclass members did not authorize Defendants' disclosure and release of their Personal Information that occurred in the Data Breach and the dissemination of their Personal Information was not done pursuant to any of the CMIA's exceptions permitting disclosure.

278. Defendants' negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and California Subclass members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA, Cal. Civ. Code §§ 56.06 and 56.101(a). The Defendant Anesthesiology Providers transmitted patients' confidential medical information to Somnia. That information was then accessed, viewed, and exfiltrated by an unauthorized third party or parties, and thus Defendants negligently released medical information concerning Plaintiffs and California Subclass members. Accordingly, Defendants' systems and protocols did not protect and preserve the integrity of electronic medical information in violation of the CMIA, Cal. Civ. Code § 56.101.

279. Defendants violated the CMIA by negligently (1) failing to implement reasonable administrative, physical and technical safeguards to protect, secure and prevent the unauthorized access to, and acquisition of, Plaintiffs' and California Subclass members' Personal Information;

(2) failing to implement reasonable data security measures, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs' and California Subclass members' Personal Information; (3) failing to use reasonable authentication procedures to track Personal Information in case of a security breach; and (4) allowing undetected and unauthorized access to servers, networks and systems where Plaintiffs' and California Subclass members' Personal Information was kept.

280. Defendants' failure to implement adequate data security measures to protect the Personal Information of Plaintiffs and California Subclass members was a substantial factor in allowing unauthorized parties to access Somnia's computer systems and acquire the Personal Information of Plaintiffs and California Subclass members.

281. As a direct and proximate result of Defendants' violation of the CMIA, Defendants allowed the Personal Information of Plaintiffs and California Subclass members to: (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be accessed and acquired by unauthorized parties in order to view, mine, exploit, use, and/or profit from their Personal Information, thereby breaching the confidentiality of their Personal Information. Plaintiffs and California Subclass members have accordingly sustained and will continue to sustain actual damages as set forth above.

282. Plaintiffs and California Subclass members were injured and have suffered damages, as described above, from Defendants' unauthorized release of their medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and are therefore entitled to nominal damages of one thousand dollars (\$1,000) for each violation under Civil Code § 56.36(b)(1) or the amount of actual damages, if any, for each violation under Civil Code § 56.36(b)(2).

283. Plaintiffs and California Subclass members also seek reasonable attorneys' fees and

costs under applicable law including Federal Rule of Civil Procedure 23, California Civil Code § 56.35, and California Code of Civil Procedure § 1021.5.

COUNT 6

CALIFORNIA UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code §§ 17200, et seq.

**On Behalf of California Plaintiffs against Somnia
and on behalf of each Defendant Anesthesiology Provider-Specific Subclass Representative
against each applicable Defendant Anesthesiology Provider**

284. The California Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

285. Defendants are “persons” as defined by Cal. Bus. & Prof. Code § 17201.

286. Defendants violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* (“UCL”) by engaging in unlawful, unfair, and deceptive business acts and practices.

287. Defendants’ “unfair” and “fraudulent” acts and practices include omitting, suppressing, and concealing the material fact that they did not have and did not reasonably ensure that Somnia reasonably or adequately secured Plaintiffs’ and California Subclass members’ Personal Information.

288. Defendants engaged in “unlawful” business practices by violating multiple laws, including California’s Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California’s Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, HIPAA, and California common law.

289. Defendants engaged in acts of deception and false pretense in connection with their accepting, collecting, securing, and otherwise protecting patient Personal Information and engaged in the following deceptive and unconscionable trade practices, including:

- a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and California Subclass members' Personal Information;
- b. Failing to comply with industry standard data security standards during the period of the Data Breach;
- c. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;
- d. Failing to adequately monitor and audit the data security systems of its vendors and business associates like Somnia;
- e. Failing to adequately monitor, evaluate, and ensure the security of Somnia's network and systems;
- f. Failing to recognize in a timely manner that Plaintiffs' and other California Subclass members' Personal Information had been compromised; and
- g. Failing to timely and adequately disclose that Plaintiffs' and California Subclass members' Personal Information had been improperly acquired or accessed.

290. Plaintiffs' and California Subclass members' Personal Information would not have been compromised but for Defendants' wrongful and unfair breach of its duties.

291. Defendants' failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and California Subclass members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and California Subclass members' Personal Information.

292. Plaintiffs and California Subclass members conferred a benefit on Defendants—payment for medical services—in reliance on Defendants' omissions and deceptive, unfair, and

unlawful practices. Had Defendants disclosed in any form, whether verbally, in writing, or via electronic disclosure that they did not adequately secure patients' Personal Information, Plaintiffs and California Subclass members would not have sought or purchased services from Defendants.

293. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass members were injured and lost money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein.

294. Plaintiffs and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their Personal Information; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 7

CALIFORNIA CONSUMER LEGAL REMEDIES ACT **Cal. Civ. Code §§ 1750, et seq.**

**On Behalf of California Plaintiffs against Somnia
and on behalf of each Defendant Anesthesiology Provider-Specific Subclass Representative
against each applicable Defendant Anesthesiology Provider**

295. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

296. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

297. Defendants are “persons” as defined by Civil Code §§ 1761(c) and 1770, and have provided “services” as defined by Civil Code §§ 1761(b) and 1770.

298. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from “[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have.”

299. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from “[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another.”

300. Plaintiffs and California Subclass members are “consumers” as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a “transaction” as defined by Civil Code §§ 1761(e) and 1770.

301. Defendants’ acts and practices were intended to and did result in the sales of products and services to Plaintiffs and California Subclass members in violation of Civil Code § 1770, including, but not limited to omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs’ and California Subclass members’ Personal Information.

302. Defendants’ omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers’ Personal Information.

303. Plaintiffs and California Subclass members conferred a benefit on Defendants—payment for medical services—in reliance on Defendants’ omissions. Had Defendants disclosed in any form, whether verbally, in writing, or via electronic disclosure that they did not reasonably

adequately secure patients' Personal Information, Plaintiffs and California Subclass members would not have sought or purchased services from Defendants.

304. Had Defendants disclosed to Plaintiffs and California Subclass members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced employ systems with reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and California Subclass members' Personal Information as part of the services they provided without advising Plaintiffs and California Subclass members that their data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and California Subclass members' Personal Information. Accordingly, Plaintiffs and California Subclass members acted reasonably in relying on Defendants' omissions, the truth of which they could not have discovered.

305. As a direct and proximate result of Defendants' violations of California Civil Code § 1770, Plaintiffs and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

306. Plaintiffs and California Subclass members have provided notice of their claims for damages to Defendants in compliance with California Civil Code § 1782(a) and intend to amend

this Complaint to seek statutory damages against all Defendants following a ruling on a motion to dismiss, in compliance with the relevant notice requirements.⁴⁶

307. Plaintiffs and California Subclass members seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COUNT 8

CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, et seq.

**On Behalf of California Plaintiffs against Somnia
 and on behalf of each Defendant Anesthesiology Provider-Specific Subclass Representative
 against each applicable Defendant Anesthesiology Provider**

308. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

309. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.2. The disclosure must "be made in the most expedient time possible and without unreasonable delay," *id.*, but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82,

⁴⁶ Plaintiffs provided notice of their claims for damages to AS-San Joaquin and Somnia on December 13, 2022. AS-San Joaquin and Somnia failed to cure within 30 days and Plaintiffs therefore seek statutory damages under the CLRA against AS-San Joaquin and Somnia. On February 28, 2023, Plaintiffs provided notice of their claims for damages to the remaining Defendants—Palm Springs-AS, RAA-IL, RAA-NM, and AA-El Paso.

subdiv. b.

310. The Data Breach constitutes a “breach of the security system” of Defendants.

311. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the California Subclass.

312. Defendants knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the California Subclass, but waited more than three months to notify them.

313. Three months was an unreasonable delay under the circumstances.

314. Defendants’ unreasonable delay prevented Plaintiffs and California Subclass members from taking appropriate measures to protect themselves against harm.

315. Because Plaintiffs and California Subclass members were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

316. Plaintiffs and the California Subclass are entitled to equitable relief and damages in an amount to be determined at trial.

REQUESTS FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class, as applicable, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

a. Certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs’ counsel as Class Counsel;

b. Grant permanent declaratory and injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

c. Award Plaintiffs and the Class equitable, injunctive, and declaratory relief,

as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Somnia from experiencing another data breach by adopting and implementing best data security practices to safeguard Personal Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

d. Award Plaintiffs and Class Members compensatory, consequential, and general damages in an amount to be determined by a jury at trial;

e. Order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

f. Award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

g. Award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

h. Award pre- and post-judgment interest at the maximum legal rate; and

i. Grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: March 1, 2023

By: /s/ Jason L. Lichtman

Jason L. Lichtman
Sean A. Petterson
Margaret J. Mattes
**LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP**
250 Hudson Street, 8th Floor
New York, New York 10013
Telephone: 212.355.9500
Email: jllichtman@lchb.com
spetterson@lchb.com
mmattes@lchb.com

By: /s/ Todd S. Garber

Todd S. Garber
Andrew C. White
**FINKELSTEIN, BLANKINSHIP,
FREI-PEARSON & GARBER, LLP**
One North Broadway, Suite 900
White Plains, NY 10601
Telephone: 914-298-3284
Email: tgarber@fbfglaw.com
awhite@fbfglaw.com

Michael W. Sobol (admitted *pro hac vice*)

**LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP**
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000
Email: msobel@lchb.com